TO: USPTO

ZILKA-KOTAB
PC
ZILKA, KOTAB & FEECE™

100 PARK CENTER PLAZA, SUITE 300
SAN JOSE, CA 95113

TELEPHONE (408) 971-2573
FAX (408) 971-4660

FAX COVER SHEET

Date:	November 20, 2006	**Phone Number**	**Fax Number**
To:	Examiner C. Laforgia		(571) 273-8300
From:	Kevin J. Zilka		

Docket No.: NAI1P089_00.175.01 **App. No: 09/836,214**

Total Number of Pages Being Transmitted, Including Cover Sheet: 11

Message:

Please deliver to Examiner C. Laforgia.

Thank you,

Kevin J. Zilka

☐ *Original to follow Via Regular Mail* X *Original will Not be Sent* ☐ *Original will follow Via Overnight Courier*

IF YOU DO NOT RECEIVE ALL PAGES OR IF YOU ENCOUNTER
ANY OTHER DIFFICULTY, PLEASE PHONE April
AT (408) 971-2573 AT YOUR EARLIEST CONVENIENCE

November 16, 2006

RECEIVED
CENTRAL FAX CENTER

NOV 2 0 2006

Doc Code: AP.PRE.REQ

PTO/SB/33 (07-05)
Approved for use through xx/xx/200x. OMB 0651-00xx
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

PRE-APPEAL BRIEF REQUEST FOR REVIEW

Docket Number (Optional)
NAI1P089/00.175.01

I hereby certify that this correspondence is being transmitted via fascimile to the Commissioner for Patents, Alexandria, VA 22313-1450 to fax number (571) 273-8300.

on November 20, 2006

Signature April Skovmand

Typed or printed name April Skovmand

Application Number	Filed
09/836,214	04/18/2001

First Named Inventor: Peter T. Dinsmore

Art Unit	Examiner
2131	Laforgia, Christian A.

Applicant requests review of the final rejection in the above-identified application. No amendments are being filed with this request.

This request is being filed with a notice of appeal.

The review is requested for the reason(s) stated on the attached sheet(s).
Note: No more than five (5) pages may be provided.

I am the

- ☐ applicant/inventor.
- ☐ assignee of record of the entire interest. See 37 CFR 3.71. Statement under 37 CFR 3.73(b) is enclosed. (Form PTO/SB/96)
- ☑ attorney or agent of record. Registration number 41,429
- ☐ attorney or agent acting under 37 CFR 1.34. Registration number if acting under 37 CFR 1.34 _____

Signature

Kevin J. Zilka

Typed or printed name

408-971-2573

Telephone number

11/20/06

Date

NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required. Submit multiple forms if more than one signature is required, see below*.

☑ *Total of 1 forms are submitted.

REMARKS

The Examiner has rejected Claims 1-6, 8-16, 19-21, and 40 under 35 U.S.C. 102(e) as being anticipated by Gundavelli et al. (U.S. Patent No. 6,941,457). In addition, the Examiner has rejected Claims 28-30 under 35 U.S.C. 102(e) as being anticipated by Dondeti et al. (U.S. Patent No. 6,240,188). Further, the Examiner has rejected Claims 38 and 39 under 35 U.S.C. 102(e) as being anticipated by Kandansky et al. (U.S. Patent No. 6,295,361). Applicant respectfully disagrees with such rejections.

With respect to independent Claim 1, the Examiner has relied on Col. 5, lines 47-63; and Col. 11, lines 6-39 from Gundavelli to make a prior art showing of applicant's claimed technique "wherein said updating does not use new secret information."

Applicant respectfully asserts that the above excerpts cited by the Examiner actually *teach away* from applicant's specific claim language. In particular, Gundavelli discloses that "upon determining that a first departing member has left the second multicast group a private multicast group non-zero random integer is selected." Further, Gundavelli discloses that "[a] second multicast group exchange key is then generated based on a private multicast group non-zero random integer, a public non-zero integer and a public prime integer."

Thus, in Gundavelli when a member has left a group, new secret information is utilized in creating the exchange key, including "a private multicast group non-zero random integer, a public non-zero integer and a public prime integer," as expressly disclosed. Applicant, on the other hand, claims that the "updating does not use new secret information" (emphasis added), as claimed.

In the Office Action mailed 07/24/06, the Examiner "interpreted secret as key, and new secret information as generating a new key." Further, the Examiner argued that "[a]s Gundavelli states in the cited sections that a new group key is generated using the traditional Diffie-Hellman approach, which is to generate a group key using the members

already existing keys...[and that t]herefore, Gundavelli discloses updating a secret without using new secret information."

Applicant respectfully disagrees and points out the steps of the traditional Diffie-Hellman approach, as found in the Gundavelli reference:

> "A known public key exchange method is the Diffie-Hellman algorithm described in U.S. Pat. No. 4,200,770. The Diffie-Hellman method relies on the difficulty associated with calculating discrete logarithms in a finite field. According to this method, two participants, A and B, **each select random large numbers a and b, which are kept secret.** A and B also agree (publicly) upon a base number p and a large prime number q, such that p is primitive mod q. A and B exchange the values of p and q over a non-secure channel or publish them in a database that both can access. Then A and B each privately compute public keys A and B, respectively..." (Col. 3, lines 5-16 - emphasis added)

As emphasized in the above excerpt, the Diffie-Hellman approach requires that the participants "each select random large numbers a and b, which are kept secret" (emphasis added). Furthermore, Gundavelli states that "the remaining members within multicast group 330 may establish a new secret key using the traditional Diffie-Hellman algorithm" (Col. 11, lines 3-35) and that "according to [the Diffie-Hellman] method, each [of the participants] select random large numbers a and b, which are kept secret" (emphasis added). Thus, in Gundavelli, when a member has left a group, new secret information, namely random large numbers, are utilized in creating the new secret key. Applicant, on the other hand, claims that the "updating does not use new secret information" (emphasis added), as claimed. Clearly, utilizing new secret information when a member leaves the group *teaches away* from "not us[ing] new secret information" (emphasis added), as claimed by applicant.

Further, with respect to independent Claim 28, the Examiner has relied on Col. 8, line 43 to Col. 9, line 19 from the Dondeti reference to make a prior art showing of applicant's claimed technique "wherein said update does not include new secret information."

Applicant respectfully asserts that the excerpt from Dondeti relied upon by the Examiner merely discloses that "[w]hen a member 22 leaves, its neighbor initiates the rekeying process" and that "[i]t sends the new keys to the members of its key association group and they are responsible for propagating the new keys to the appropriate members in their subgroups" (emphasis added). However, the mere disclosure that new keys are sent to the members of the group when a member leaves, as in Dondeti, simply fails to specifically suggest a claimed technique "wherein said update does not include new secret information" (emphasis added), as claimed by applicant.

With respect to independent Claims 38 and 39, the Examiner has relied on Col. 1, line 66-Col. 2, line 61 in Kadansky to make a prior art showing of applicant's claimed technique "wherein said update does not include new secret information." Applicant respectfully asserts that such excerpt, along with the entire Kadansky reference, only relates to a method of distributing a new group key, but does not even suggest how such new group key is created. Thus, simply nowhere in Kadansky is there any teaching of an "update [that] does not include new secret information" where such update is used for updating "at least one compromised secret known by at least one evicted user" (emphasis added), in the context claimed by applicant.

With respect to independent Claim 13, the Examiner has again relied on Col. 5, lines 47-63; and Col. 11, lines 6-39 from Gundavelli to make a prior art showing of applicant's claimed technique "wherein said determining uses a function having the following properties: (1) knowledge of said updated first key does not give knowledge of said first key or said second key, (2) knowledge of said first key does not give any knowledge of said updated first key, and (3) knowledge of said first key and said updated first key does not give any knowledge of said second key."

Applicant respectfully asserts that simply nowhere in Gundavelli is there any disclosure that "knowledge of said first key and said updated first key does not give any knowledge of said second key," as specifically claimed by applicant. In fact, applicant notes that such excerpts only disclose utilizing random integers to create an updated key

(see emphasized except above) and using the traditional Diffie-Hellman algorithm to create a new shared secret key. Clearly, such teachings do not even suggest that "knowledge of said first key and said updated first key does not give any knowledge of said second key," as specifically claimed by applicant.

In the Office Action mailed 07/24/06, the Examiner argued that "[a]pplicant claims descriptive material that is the reasoning behind updating the compromised key, [that] it allows for the updating of the group key without compromising any member of the group's key...[and that t]herefore, Gundavelli discloses knowledge of the first key and updated first key does not give any knowledge of said second key, thereby making the keys resistant to collusion attacks."

Applicant respectfully disagrees and asserts that in Gundavelli, a new secret key (i.e. third shared secret key) is generated for a group in which a member has left. The new secret key is generated utilizing an exchange key that is based on integers (i.e. non-zero random integer, public non-zero integer, and public prime integer) and a second shared secret key that was used by the group that included the member that left (see particularly Col. 5 of Gundavelli). Thus, in Gundavelli, knowledge of the new secret key inherently includes knowledge of the second shared key since the members are the same except for the member that left. Therefore, Gundavelli *teaches away* from applicant's claimed "knowledge of said first key and said updated first key does not give any knowledge of said second key" (emphasis added), as specifically claimed by applicant.

The Examiner is reminded that a claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described in a single prior art reference. *Verdegaal Bros. v. Union Oil Co. Of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). Moreover, the identical invention must be shown in as complete detail as contained in the claim. *Richardson v. Suzuki Motor Co.* 868 F.2d 1226, 1236, 9USPQ2d 1913, 1920 (Fed. Cir. 1989). The elements must be arranged as required by the claim. This criterion has simply not been met by any of the references relied on by the Examiner, as noted above.

Applicant further notes that the prior art is also deficient with respect to the dependent claims. Just by way of example, with respect to Claim 7, as rejected under 35 U.S.C. 103(a) as being unpatentable over Gundavelli in view of Takeda (U.S. Patent No. 6,178,244), the Examiner has relied on Col. 12, lines 38-43 in Takeda to make a prior art showing of applicant's claimed technique "wherein said updating occurs on a periodic basis." Applicant respectfully asserts that such excerpt relied on by the Examiner does not teach updating at least one compromised secret "on a periodic basis," in the context claimed by applicant. Instead, Takeda only discloses updating a session key in response to certain circumstances, namely "right after receiving the session key," "when the communication is interrupted," and "when a predetermined time period has passed after receiving the session key." Clearly, such circumstances do not meet any sort of periodic basis, in the context as claimed by applicant.

Additionally, with respect to Claim 40, the Examiner has relied on Col. 11, lines 6-39 of the Gundavelli reference to make a prior art showing of applicant's claimed technique "wherein said non-compromised secret utilized for said updating is known by all users in said plurality of users and is not known by said at least one evicted user."

Applicant respectfully asserts that the excerpt from Gundavelli relied upon by the Examiner merely discloses that "when a member leaves the multicast group, a new shared secret key is generated for communicating between those members that remain in the multicast group" (emphasis added). Further, Gundavelli discloses that "when a person leaves the group, a new shared secret key is established using the traditional Diffie-Hellman algorithm" and "[t]he remaining members may then use the newly established shared secret key to securely communicate with each other" (emphasis added). However, the mere disclosure that when a member leaves a group, a new shared secret key is generated for the remaining members to securely communicate simply fails to even suggest the use of a non-compromised secret, much less a "non-compromised secret [that is] utilized for said updating is known by all users in said plurality of users and is not known by said at least one evicted user" (emphasis added), as claimed.